	Application No.	Applicant(s)
Notice of Allowability	09/670,424	SATO ET AL.
	Examiner	Art Unit	
	Pramila Parthasarathy	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *12/21/2005*.

2. ☒ The allowed claim(s) is/are *30,33,34,37,38 and 40-42; Renumbered as 1-8*.

3. ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a) ☒ All   b) ☐ Some*   c) ☐ None of the:

        1. ☒ Certified copies of the priority documents have been received.

        2. ☐ Certified copies of the priority documents have been received in Application No. _____ .

        3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

    * Certified copies not received: _____ .

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.

    (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached

        1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____ .

    (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of

       Paper No./Mail Date _____ .

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)

2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)

3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____

4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material

5. ☐ Notice of Informal Patent Application (PTO-152)

6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .

7. ☒ Examiner's Amendment/Comment

8. ☒ Examiner's Statement of Reasons for Allowance

9. ☐ Other _____ .

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

DETAILED ACTION

1.   Applicant's amendments to specification filed on December 21, 2005 has been

entered and made of record.

Claim Rejections - 35 USC § 112

2.   The rejection of Claims 30, 33, 34, 37, 38 and 40 – 42 under 35 U.S.C. 112,

second paragraph has been withdrawn.

Allowable Subject Matter

2.   Claims 30, 33, 34, 37, 38 and 40 – 42 are allowed.

3.   The following is an examiner's statement of reasons for allowance: The Admitted

prior art Goldstein U.S. Patent 5,963,642 and Taguchi, disclose a method for encrypting

database information such that the data can be directly processed while still in an

encrypt form and a data processing apparatus with software protecting functions

capable of enhancing the level of encryption security independently of the memory

management by encrypting the received data using an encryption key and the

encrypted data is placed in a storage unit. Goldstein further discloses internal level

database information is located remotely from users in the form of property-oriented

positional q-code suitable for directly performing database information and Taguchi

further discloses a decryption unit decrypting the encrypted data using the decryption

key.

However, the admitted prior arts do not disclose, teach or suggest "a key

specification storing unit that memorizes data specifying a type of encryption system to

be used to encrypt data segments of each column of a database, if the column of the

database is to be encrypted; a first encryption unit that encrypts in accordance with the

data stored by the key specification storing unit: (i) data segments forming data

segment groups corresponding to column item category titles of a first kind using a

same column key, and (ii) data segments forming data segment groups corresponding

to column item category titles of a second kind, in units of rows of the database, using

row keys respectively specified for each of the rows, said item category titles identifying

respective categories of the data segments; a second encryption unit that encrypts,

using a basic key, all of the row keys used by the first encryption unit; a key data

generating unit that generates the column key, the row keys and the basic key; a storing

operation unit which stores in a memory the database after encryption by the first

encryption unit and the row keys after encryption by the second encryption unit, in a

mutually associated manner; wherein the row keys are each generated based on a

number of the respective rows and a random number; wherein a vector generation unit

sequentially generates vector confined to a closed subspace of an n-dimensional space

and defined by functions based on the keys; and wherein a logical operation unit

performs a logical operation in units of a bit involving both the data segments of the
database and components of the vectors generated by the vector generation unit, to
encrypt the data segments".

4.   Any comments considered necessary by applicant must be submitted no later
than the payment of the issue fee and, to avoid processing delays, should preferably
accompany the issue fee. Such submissions should be clearly labeled "Comments on
Statement of Reasons for Allowance."

5.   An examiner's amendment to the record appears below. Should the changes
and/or additions be unacceptable to applicant, an amendment may be filed as provided
by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be
submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview
with Douglas Holtz, registration number 33,902 on January 26, 2006. In addition, Claim
40 recites that the row keys and at least one of the column keys specify constants of the
functions, in accordance with the disclosure in the specification at, for example, page
133, line 14 – 18.

IN THE CLAIMS:

30.   (Amended)   A database management apparatus comprising:

a database storage unit which stores a database comprising a plurality of records

each record including a plurality of data segments identified by item category titles that

identify respective categories of the data segments;

an item title storing unit for storing at least one item category title for specifying a

corresponding at least one data segment group as a target of a data search process;

a key data storing unit for storing keys for use in encryption associated with the

database, wherein the keys comprise a column key corresponding to the at least one

data segment group specified by the at least one stored item category title, and a

plurality of different row keys corresponding respectively to the records of the database;

~~and~~

an encryption unit for encrypting: (i) the data segments of said at least one

specified data segment group using the corresponding column key, and (ii) data

segments of at least one data segment group corresponding to item category titles other

than the stored item category titles, in units corresponding to the records, using the

different row keys of the respective records;

a functional unit which encrypts a received data set comprising a search process

condition using the corresponding column key; and

a database search unit which performs the data search process by comparing

the encrypted search process condition with the encrypted data segments of said at

least one specified group;

wherein the encryption unit sequentially generates vectors in a multidimensional

space based on a set of predetermined functions, and the data segments are encrypted

in accordance with an encryption method in which components of the sequentially

generated vectors form a key stream of a key associated with the encryption method;

and

wherein the row keys and the column key specify constants of the functions.

31 and 32.   (Cancelled)

33.   (Amended)   A database system comprising a first information processor

terminal storing a database, and a second information processor terminal which is

connected to the first information processor terminal via a network and which is adapted

to send a request to the first information processor terminal for conducting a search

process in the database, wherein the first information processor terminal comprises:

a functional unit which encrypts: data segments forming data segment groups

corresponding to column item category titles of a first kind using a column key common

to the data segment groups and, data segments forming data segment groups

corresponding to column item category titles of a second kind, in units of rows of data

segments, using respective row keys, said item category titles identifying respective

categories of the data segments;

wherein the second information processor terminal comprises:

a transmitting unit which transfers via the network, an encrypted data set

representing conditions to be used for the search process in the first information

processor terminal, when the second information processor terminal requests the first

information processor terminal to perform the search process on the database, said

encrypted data set being formed by encrypting an input data set specifying the

conditions of the search process by using the column key; ~~and~~

wherein the first information processor terminal further comprises :

a search performing unit that performs the search process on the encrypted

database, based on the transmitted encrypted data set; and

a returning unit that returns an encrypted result data set resulting from the search

process, to the second information processing terminal via the network;

wherein the encryption unit sequentially generates vectors in a multidimensional

space based on a set of predetermined functions, and the data segments are encrypted

in accordance with an encryption method in which components of the sequentially

generated vectors form a key stream of a key associated with the encryption method;

and

wherein the row keys and the column key specify constants of the functions.

34.   (Amended)   A database management apparatus comprising:

a key specification storing unit that memorizes data specifying a type of

encryption system to be used to encrypt data segments of each column of a database, if

the column of the database is to be encrypted;

a first encryption unit that encrypts in accordance with the data stored by the key

specification storing unit: (i) data segments forming data segment groups corresponding

to column item category titles of a first kind using a same column key, and (ii) data

segments forming data segment groups corresponding to column item category titles of

a second kind, in units of rows of the database, using row keys respectively specified for

each of the rows, said item category titles identifying respective categories of the data

segments;

a second encryption unit that encrypts, using a basic key, all of the row keys

used by the first encryption unit;

a key data generating unit that generates the column key, the row keys and the

basic key;

a storing operation unit which stores in a memory the database after encryption

by the first encryption unit and the row keys after encryption by the second encryption

unit, in a mutually associated manner;

wherein the row keys are each generated based on a number of the respective

rows and a random number;

wherein a vector generation unit sequentially generates vector confined to a

closed subspace of an n-dimensional space and defined by functions based on the

keys; and

wherein a logical operation unit performs a logical operation in units of a bit

involving both the data segments of the database and components of the vectors

generated by the vector generation unit, to encrypt the data segments.

35 and 36.   (Cancelled)

37.   (Amended)   A method for managing a database system including a first terminal

unit for managing the database and a second terminal unit for searching the database

independently of the first terminal unit, said method comprising:

encrypting the database by encrypting, on a first terminal side of the system:(i)

data segments forming data segment groups corresponding to column item category

titles of a first kind using a same column key, (ii) data segments forming data segment

groups corresponding to column item category titles of a second kind, in units of rows of

the database, using Low keys respectively specified for each of the rows, and (iii) all of

the row keys, using another key, said item category titles identifying respective

categories of the data segments;

storing, at the first terminal unit side of the system, the encrypted database on

portable storage medium units for distribution; and

searching the encrypted database stored on any of the distributed storage

medium units, decrypting a data set obtained as a search result and displaying the

decrypted data set at a second terminal unit side of the system;

wherein the row keys are each generated based on a number of the respective

rows and a random number;

wherein a vector generation unit sequentially generates vector confined to a

closed subspace of an n-dimensional space and defined by functions based on the

keys; and

wherein a logical operation unit performs a logical operation in units of a bit

involving both the data segments of the database and components of the vectors

generated by the vector generation unit, to encrypt the data segments.

39.   (Cancelled)

40.   (Amended)   A database management apparatus, comprising:

a database storage unit which stores a database comprising a plurality of records

each record including a plurality of data segments identified by item category titles that

identify respective categories of the data segments;

an item title storing unit for storing at least one item category title for specifying a

corresponding at least one data segment group as a target of a data search process;

a key data storing unit for storing keys for use in encryption associated with the

database, wherein the keys comprise a column key corresponding to the at least one

data segment group specified by the at least one stored item category title, and a

plurality of different row keys corresponding respectively to the records of the database;

and

an encryption unit for encrypting: (i) the data segments of said at least one

specified data segment group using the corresponding column key, and (ii) data

segments of at least one data segment group corresponding to item category titles other

than the stored item category titles, in units corresponding to the records, using the

different row keys of the respective records, using the different row keys corresponding

to the respective records and another column key that is assigned commonly to the data

segment groups corresponding to item category titles other than the at least one stored

item category title;

wherein the encryption unit sequentially generates vectors in a multidimensional

space based on a set of predetermined functions, and the data segments are encrypted

in accordance with an encryption method in which components of the sequentially

generated vectors form a key stream of a key associated with the encryption method;

and

wherein the row keys and at least one of the column keys specify constants of

the functions.

41.   (Amended)   A computer program for directing a computer to execute functions

comprising:

accessing a database comprising a plurality of records, each record including a

plurality of data segments identified by item category titles that identify respective

categories of the data segments;

storing at least one item category title for specifying a corresponding at least one

data segment group as a target of a data search process;

storing keys or use in encryption associated with the database, wherein the keys

comprise a column key corresponding to said at least one data segment group specified

by the at least one stored item category title, and a plurality of different row keys

corresponding respectively to the records of the database;

encrypting: (i) the data segments of said at least one specified data segment

group that is the target of the data search process using the column key corresponding

to the at least one specified data segment group, and (ii) data segments of at least one

data segment group corresponding to item category titles other than the at least the

stored item category titles, in units corresponding to the records, using the different row

keys of the respective records;

wherein the encryption unit sequentially generates vectors in a multidimensional

space based on a set of predetermined functions, and the data segments are encrypted

in accordance with an encryption method in which components of the sequentially

generated vectors form a key stream of a key associated with the encryption method;

and

wherein the row keys and the column key specify constants of the functions.

42.   (Amended)   A computer program for directing a computer to execute functions

comprising:

storing data specifying a type of encryption system to be used to encrypt data

segments of each column of a database, if the column of the database is to be

encrypted;

first encrypting in accordance with the data stored by the key specification

memory: (i) data segments forming data segment groups corresponding to column item

category titles of a first kind using a same column key for said data segments forming

the segment groups, and (ii) data segments forming data segment groups

corresponding to column item titles of a first kind using a same column key, and data

segments forming data segment groups corresponding to column item titles of a second

kind, in units of rows of the database, using row keys respectively specified for each of

the rows, said item category titles identifying respective categories of the data

segments;

second encrypting, with a basic key, all the row keys; and

storing in a memory the database after the encryption thereof and the row keys

after encryption the encryption thereof, in a mutually associated manner;

wherein the row keys are each generated based on a number of the respective

rows and a random number;

wherein a vector generation unit sequentially generates vector confined to a

closed subspace of an n-dimensional space and defined by functions based on the

keys; and

wherein a logical operation unit performs a logical operation in units of a bit

involving both the data segments of the database and components of the vectors

generated by the vector generation unit, to encrypt the data segments.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Pramila Parthasarathy whose telephone number is 571-272-3866. The examiner can normally be reached on Tuesday – Thursday 8:00a.m. To 3:00p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-232-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR only. For more information about the PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Pramila Parthasarathy
January 26, 2005.

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100